REMARKS

Drawing Objection

The Office Action Summary does not indicate whether the drawings are accepted or objected to. As discussed in the response filed April 22, 2009, the specification was amended to eliminate the objection to the drawings. As such, it is respectfully requested that the objection to the drawings be withdrawn and that the Office Action Summary be marked accordingly.

Claim Rejections

Claims 2-23 stand rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent No. 7,260,834 (Carlson) in view of U.S. Patent No. 6,393,563 (Maruyama et al.) and U.S. Patent Publication No. 2002/0068631 (Raverdy et al.).

Claim Amendments

Claims 1, 10, and 21 are amended.

The Cited References

Carlson is directed to a gaming system 100 including a gaming server 110 that is connected to a plurality of gaming machines 120-124 via a network bus 130. (Col. 4, lines 5-8). A gaming machine encrypts information using a key 160 and transmits the encrypted information over the network bus 130. The encrypted information is transmitted to the gaming server 110 or to another one of the gaming machines. (Col. 6, lines 12-20).

Maruyama et al. is directed to a digital signature system that employs a temporary digital ID signed using a private key, so that the digital ID can be used as a proxy for a specific period of time and for a specific purpose. When a signature is requested by a server application, a user does not use his or her private key, but employs a temporary key generated using the private key. (Abstract). At the server, a hash value of the temporary certificate is acquired and is signed using the private key. (Col. 6, lines 5-7). To approve this signature, the hash value of the temporary certificate is calculated, and the result is compared with the signature decoded by the user's public key. (Col. 6, lines 7-10).

Raverdy et al. is directed to an electronic system including one or more user devices 114 and an event server 138. (¶[0031). The user devices 114 may be portable wireless telecommunication devices. (¶[0032). In one embodiment, one or more winners may be identified, and award certificates created and encrypted. The award certificates are transmitted

to the appropriate user devices 114. (¶0082). An award certificate may include owner information, certificate usage history, certificate transfer history, certificate description, security information, and data. (¶0083).

Applicants' Claimed Invention Would Not Have Been Obvious

The following factual inquiries must be considered in any obviousness evaluation: the scope and content of the prior art, the differences between the claimed invention and the prior art, the level of ordinary skill in the pertinent art and evidence of any secondary considerations. To establish a *prima facie* case of obviousness, it is axiomatic that the prior art, either alone or in combination, must disclose each and every element of the claimed invention. As stated in the M.P.E.P., "[t]o reject a claim. . . Office personnel must articulate the following: (1) a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference." M.P.E.P. §2143A.

Moreover, "[t]he rationale to support a conclusion that the claim would have been obvious is that all claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art." Id. Also, some articulated reasoning with rational underpinnings must be provided to support a *prima facie* case of obviousness.

It is respectfully submitted that claims 2-23 would not have been obvious in view of Carlson, Maruyama, and Raverdy et al.

By way of example, claim 2 recites encrypting a server-initiated message on the network at a server with a key pair. The key pair is generated using a setup key stored both in memory associated with the server and in memory associated with a gaming machine. The setup key is removed from the memory associated with the gaming machine after generation of the key pair.

The Office Action states: "Carlson is silent in regards to a setup key to generate the key pair and the setup key is removed from the memory associated with the gaming machine after generation of the key pair; and paying an award responsive to the message." (Page 3, lines 6-8). Therefore, Carlson fails to disclose or suggest encrypting a message with a key pair that is generated using a setup key stored both in memory associated with the server and in memory associated with a gaming machine wherein the setup key is removed from the memory associated with the gaming machine after generation of the key pair.

The Office Action cites Maruyama as disclosing or suggesting "a setup key to generate the key pair and the setup key is removed from the memory associated with the device after the generation of the key pair." (Page 3, lines 9-11). However, the key described in Maruyama is entirely different than the setup key recited in the claims.

Maruyama relates generally to "public key cryptography." (Col. 1, lines 7-8). Public key cryptography involves the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Indeed, Maruyama makes clear that while a message is encrypted using a temporary key generated by a client's private key (Col. 5, lines 45-47), the message is decrypted using the client's public key. (Col. 6, lines 7-10). Thus, although the private key described in Maruyama is used to generate the client's temporary key, Maruyama fails to disclose or suggest that the private key is used to generate the key possessed by the message recipient (i.e. the client's public key). Therefore, the private key described in Maruyama is only used to generate a single key, not a key pair as recited in claim 2.

Further, Maruyama fails to disclose or suggest that the private key is possessed by the message recipient. Instead, possession of the private key is limited to the client. (Col. 5, line 65, through col. 6, line 23). That is, messages sent by the client are encrypted with the private key at the client and decrypted with the public key at the message recipient. (Col. 1, lines 11-59). Since the private key described in Maruyama is not possessed by the message recipient, it is not "stored both in memory associated with the server and in memory associated with a gaming machine," as recited in claim 2.

Therefore, Maruyama fails to disclose or suggest a setup key that is "removed from the memory associated with the gaming machine after generation of the key pair" as recited in claim 2, since the private key described in Maruyama is neither used to generate a key pair nor "stored both in memory associated with the server and in memory associated with a gaming machine wherein."

Raverdy et al. is not cited in the Office Action as disclosing or suggesting any feature related to a key pair generated using a setup key and, therefore, fails to disclose or suggest the same features lacking in Carlson and Maruyama.

Since claim 2 recites features not disclosed or suggested in any of the cited references, considered alone or in combination, claim 2 would not have been obvious in view of the cited references. Independent claims 10 and 21 recite features similar to those recited in claim 2. Therefore, claims 10 and 21 would not have been obvious for at least the same reasons as claim 2. The dependent claims include, by virtue of their dependency, the features of the independent

claims on which they are based. Therefore, the dependent claims would not have been obvious for at least the same reasons as their respective independent claims.

Conclusion

In view of the foregoing, it is respectfully submitted that all the claims are now in condition for allowance. Accordingly, allowance of the claims at the earliest possible date is requested.

If prosecution of this application can be assisted by telephone, the Examiner is requested to call Applicants' undersigned attorney at (510) 663-1100.

If any fees are due in connection with the filing of this amendment (including any fees due for an extension of time), such fees may be charged to Deposit Account No. 504480 (Order No. IGT1P306C1).

Dated: October 30, 2009

Respectfully submitted,

Weaver Austin Villeneuve & Sampson LLP

/William J. Egan, III/

William J. Egan, III
Reg. No. 28,411

P.O. Box 70250
Oakland, CA 94612-0250